Recap of March 11, 2004, Meeting
Information Service Policy Committee
1:00pm Room 106 County/City Building

Attendees:

Jon Camp, Dave Kroeker, Ray Stevens, Don Herz, Doug Thomas, Ken Kuszak

Administrative:

UPS;

The UPS batteries were all replaced early last week.

Backup Generator;

The electrical engineer has looked at the back up generator which is in the 233 Building that was formerly used by LPD. He is also considering the possibility of Doug Ahlberg moving into the building and his associated needs. He said it would not be a problem because I.S., which will be the biggest user, will only need about 50% of the generator's capacity. The generator will need to be modified for our use. He is getting some specifications together for us so that we can create a bid document. This generator will have enough power for our computer room, the EOC, the servers for the State Child Support Office, and probably the State Patrol's Records Department. Any additional modifications for these agencies will need to be funded by them however. We are only bidding out and paying for the portion that makes it functional for IS. There are some modifications that will need to be made to electrical lines between the floors and the electrical engineer thought it could probably cost around $20,000.
There is not a large capacity in the tank of the generator. There is a "Day" tank which is 20 gallons and a 60-gallon tank for weekends. In the case of a long term power failure we would have to make arrangements for a local fuel delivery. The only time we would use it would be for a long term outage.

Cherry Creek Facility;

The work at this facility is moving forward to accommodate our electrical needs. Gary Bergman and his staff have been really good to work with. We are now working on putting together a floor plan of classroom "C". Gary has also marked some space in the area for County Extensions equipment which he asked to be included. We will incorporate their server into our plans. This facility will be used as the Information Services back up facility in case of a disaster. Our IBM equipment takes special plugs and the floor layout we are doing will help Dave Drevo in making the cables the right length to accommodate the various plug types.
Currently, we do daily backups that are sent off-site to a facility that is protected with halon and controlled entry. As part of our Disaster Recovery Plan, we have a contract with a firm that will supply us with temporary equipment based on our current use. They ship it here and it should all arrive within 72 hours. We would then set up the equipment at the Cherry Creek facility. Historically, we have had a contract with a firm that would bring in two semi trucks that fold out into a data center. This contract is fairly costly and for less than what we pay for this contract in one year, we can modify the Cherry Creek Facility to meet our needs. The bad side is that the Cherry Creek facility is relatively close to our current location and if a tornado hit us it is possible that it could hit that building as well. However, there are a number of buildings that we have our fiber run to so in the event that both buildings were destroyed, we would probably set up at one of our other remote government sites, (ie PW on North 27th, Trabert Hall).

I.S. Remodeling;

The remodeling continues to move forward. Phase One is scheduled to be done in three more weeks. This phase is about one third of the total space that is being remodeled. Right now the remodeling

is being completed in the applications development area. Terry and his people are in the large conference room, Jim Walkenhorst and his people are in the training room and Mark Wieting and two of his people are in the War Room. Deb is using the training facilities at the Library. Phase Two will displace more people. It affects all of the PC people, all of the Tech Support people in the office area and the Administrative staff. We do not have an actual time-line for Phase Two but it will probably be minimum of a 6 to 8 week job. Hopefully, by the first of the new fiscal year the remodeling will be completed.

Networking

K Street Fiber;

Next weekend we plan to move the fiber within the conduit. Now that the melted snow/ice has gotten out of the conduit, we can pull the fiber out of it and reinstall it in the new route. The Police Garage, former Elections Building, and StarTran are the three buildings that will be impacted. As part of this relocation we have turned K Street into a major network hub. Since we had to relocate anyway we are in the process of building full redundancy within the downtown City /County campus. This will also create a redundant loop to our wireless facilities which are on the roof of the K Street complex. This wireless goes to Trabert Hall, Urban Development and the Juvenile Detention Center. Transportation also has wireless network facilities at K Street for the parking garages. In addition, if we lose the 10th street link between 233 and the Hall of Justice/County City Building connectivity won't be lost since we will be creating a redundant 9th street path in the spring.

Trabert/Mental Health and Health;

It is Doug's understanding that all of these issues have been resolved and contracts are in the process of being signed.

Fire Station #14;

Doug checked with LES, they are doing a little fiber work for us at Fire Station #14 which is also the back up 911 Center. They are getting us onto their fiber so that we can cancel the T1 line out there. This will save some money ($750/ month between the 911 Center and Fire and increase performance. As of last week when Doug talked to Bill Hansen at LES, it was still too muddy to get much done. In the next couple of weeks this should be installed and ready for testing.

Email Attachments;

Doug sent the committee members an email on email attachments. The viruses that are going around these days are getting a little more cagey with regards to their subject lines. Accordingly we are getting more of them opened on the network prior to the antidote signature files being available. What we would like to do and what other businesses in town have been doing, is figure out a way to deal with attachments. Some organizations do not allow attachments. One of the things that we have considered is to hold all attachments for four hours and then let people go to another server and grab their attachments. The virus that came in, NetSky.k, which did hit us hard came through before there was even an updated signature file to fix it. These viruses have not been destructive to the network, they have just been a nuisance, denial of service type of virus. They have not crashed hard drives or changed files, so we have been very lucky. However, we have gotten a number of them through in the last couple of weeks. The problem is, once that virus arrives on the internet, the vendors have to write the code to recognize it and it could take sometime. For instance, on Monday when the first one came into the network at 2:37 at Corrections around 5:00 the antidote was made available. This is why we are thinking that if we held all of the attachments 3 or 4 hours, those with new viruses could be identified, we could update the signature file, quarantine those off and be okay.

A second option is to require whoever is sending an email to you with an attachment to add an extension, were thinking "cty" on the end of the file name. We could then let everything with a "cty" extension through immediately (no quarantine), and so if you knew that someone was going to send you something just tell them to put a .cty at the end (through their file manager), and it will make it through the firewall. We are thinking about blocking all extensions except for .pdf or .cty. Since this would be a very unique extension and people would have to direct the virus to the city or county extension, (it would not be generally known on the internet). If you receive a .cty that is really a Microsoft word file, you will have to detach it, take the cty off. The attachment name would look like "DocumentName.doc.cty" and you would have to remove the .cty extension to open it in Word. If you were sent a document attachment from someone, who did not include the .cty on the end of the document, the intended recipient would get a message from the network saying that "This message attempted to have a document attached to it that did not carry the approved extension. Re-contact them and have them resend it with the .cty extension." This way you contact the people telling them you did not get the document attachment because the attachment did not contain the correct extension. If it is not legitimate, you can disregard the message.

These are the two alternatives that we are exploring. Some places are not allowing any attachments. From an administrative stand point, Ken and Doug both agree that the .cty extension is the easiest to do. From a staff stand point, this is going to be the hardest to do. It may have the possibility of being automatic on the four hours or twelve-hour quarantine with auto resend, but we need to explore this further. There are same cases in which people cannot wait 12 hours to receive the email and attachments which is why the .cty extension would work. You would tell people to add this to the end of the attachment and then it would go through the firewall immediately. PDF files are okay and we will let those through immediately. Doug thinks the .cty extension would be the most effective solution.

After a discussion by committee it was agreed that maybe we should look at the two tiered system, this would allow people who do not know the attachments are coming or are not aware of the need to use the .cty extension to eventually get the information and it is still faster than snail mail.

The virus software can scan the attachments for viruses but they are coming in prior to the anti virus software vendors updating the signature files. There was some porn stuff that come through, which did contain explicit words, but it was not filtered out at the firewall. The spam filter does the virus checking. It looks for code in the attachments by recognizing it by the list of subjects lines, if you went out and looked at the site they showed you the 17 subject lines this virus could contain and this is how Doug thinks the Spam filter works, by recognizing the subject line and not the actual code. Ken, however, thought it actually opened the attachment and looked at the code in it.

Don receives minutes in .doc format and this same attachment is sent to 50 people or more and rather than having to bother them to change the attachment name for one person, on these types of things, he does not care if they come 12 hours later. Don is thinking that a combination of the .cty and the quarantine of email attachments that do not have the .cty extension is the way to go. Doug will do some more investigation into what type of two tiered system we could have and will present his findings and recommendations to the committee next month. If you need something on an emergency basis you will probably take the time to contact the sender and ask them to resend the attachment using the .cty extension. If an email with an attachment was sent and was held for six hours you would receive a message that someone tried to send you an email but it did not meet security standards related to email attachments.

Doug is going to give Cori in the County Commissioner's Office and Sharon Porter some information to distribute about shutting machines down at nights. This is another issue. We had a City employee that opened a file Monday night, after we had told them to shut their machine off. They signed off the network but did not shut their machine off. Since many viruses work as "services", so as long as you are physically cabled, and the pc is powered on, then it will continue to distribute the virus, even though you are not signed onto the network. We do have a better way of getting the newest Norton signature files out to all machines throughout the day, it is not longer

necessary to have a boot up to distribute the most recent signature file.
Dave asked if there was a way to remotely power off every computer that has not been powered off? Ken said that they have been considering a policy that if someone has not shut down their machine in the last 24 to 48 hours, we could pop up a window message informing them they have two hours to shut down their PC or in two hours it will shut itself off. For Win2000 and Win XP machines we can check the domain to see if the PC has not been shut off recently. In reviewing the log we noteted that there is one person who has not shut their PC off since April of last year.
Jon Camp and Ray Stevens have both indicated that whatever it takes, make to environment secure. We need to have a good policy and be able to justify it. On Monday, when the virus' really got spread throughout the network, two of the PC's left on were in County Court. Doug reminded them that they needed to shut down their machines each night. One sent Doug a very apologetic email but the other person did not respond.

Hot Mail;
This is another security issue. Hot mail (externally managed email), uses HTTP instead of normal mail protocol, (SMTP), so if someone signs on to a Hot Mail (ie Yahoo, MSN, AOL, Net Zero, Earth Net, CompuServe), account from inside the network, our scanner does not recognize it as mail so we are totally exposed to those messages and any related attachments. We are shutting off instant messaging, the known ones like AOL, Yahoo, MSN, we have also shut of Kazaa. At one time there was a person in the Mayor's office during the Wesely Administration who said they had to have this (third party mail). There is a number of problems with it, number one it is totally out of our domain so some third party out there is totally administering and potentially has access to individual accounts, At some point in time the State is going to formally mandate requirements for the retention of email, we have no retention capabilities on the third party administered accounts. These third party administered "hot mail", accounts are employees own personal mail accounts. They go check their personal email from work. Ray said that he does it. There are about 30 third party providers that we would block and that would cut down our exposure by 99%.
People are using personal email and they should be using City email. The Lotus Notes address book is not one usually attacked by hackers. They usually attack Microsoft email systems and this is how the viruses proliferate around the world. We do have anti-virus software running on the Notes server. We are making it more cost prohibitive to not use Notes as an email service. In the past, it was more expensive to use Notes and if you had a older machine Notes does not run well. The new INotes, (the internet version of Notes), is the same price as the regular Notes account, it does not however require as thick of a client as Notes. It will run and give you the same functions as Notes. It does have a little different look. Over the long haul, Doug does see I.S. getting out of using POP3 mail accounts and having everyone use Lotus Notes or the INotes version.
The County Assessor, City Attorney, Aging and several County agencies are using POP3 mail accounts and not Notes. There is currently a $10 difference in cost per year. Notes cost $50 and POP mail costs $40. There is a $78 up front cost to purchase a Notes license. Next year Doug is thinking it will be $50 for Notes and $65 for POP. Last year it cost $25 for POP mail accounts. We have a much larger exposure with POP3 mail accounts than we do with Notes, so the costs should reflect the additional costs of controlling the exposure created by POP mail.
Version 6.5 of Notes is out and it has a new look to it. TO-DO lists in the current version are put in your calendar but the new version gives you the option not to put them on there. This version also has a chat option.

Virus activity over the last couple of weeks is at an all time high. Every day there are new viruses being spread. Dave was there when Tammy received a message from Jonathan Cook and when she opened it up and it sounded like a washing machine. They said it unleashed several viruses and her machine was down for a couple of days while they were cleaning it up. Her name is probably in Jonathon's address book which is how Tammy received it from him. It grabs two people out of an address book and sends a message to one of them and shows it as coming from the other.

We have a limited number of places using RoadRunner but all this is encrypted and we have an actual hardware device that does authentication and is part of the firewall via a VPN connection.

In terms of Administration, we have more control over identifying problems and tracking them down in the new versions of Windows than we do over the older versions. One of the viruses that came out was actually written to attack the GroupWise, (Novell), address book.
Currently, when someone tries to send us an email with a virus in it, we just send a message to the recipient that it was quarantined because a virus was detected. We are not sending a message back to the original sender that they sent a message with a virus in it.

Doug thinks that next month he will have Jeff and a couple of the tech. guys come to the meeting. Dave forwarded Doug's email about attachments to Kerry and Kerry thought that they should present this information to the County Board. Dave told him originally they should wait until after the meeting today. Dave thinks they will need to present this information to the County Board and have someone go and explain the problems and options so the Board understands before I.S. dictates any new policies. Doug feels there will be some fall out over no longer having access to "hot mail" accounts. INotes is something you can use to look at your Notes account through any Internet account. The current version of INotes is a very robust product. Notes also has Notes Everywhere installed which is wireless. Doug will contact Dave when they are ready explain this information to the County Board.

Sheriff,
We are working with the Sheriff's Office on some palm wireless application problems. They arrest a lot of people based on the information they get off of their palms in the court room. So it is important that this application meet their needs. They arrest three to four people a week. Mark is also working with them to streamline the repeat data they enter in the palm application.

Spyware,
We are putting Spybot on all new PC's . This software looks for spyware that has been installed on your machine. It is a free download. On IE, if you go to security you can set security to its highest and not allow any cookies.

Applications Development:

County Finance;
Dave said they were going to try and get the People Soft contract to the Board this month. Jim is aware of this and Dave would like to sit down with him and identify what resources they want. Dave has some problems with things like training sessions they need to do. They have a staffing plan that is pretty extensive and there could be problems freeing up the people they need. If they had not put this in the contract, he would have relied on what Mark said. However, they are stating in the contract that there needs to be a large amount of staff time committed to this project and in the summer that could be a problem. There needs to be a commitment in the various agencies and Dave would like to identify the departments. Terry Adams is looking at upgrading a position for someone to be a primary participant in the migration for the County Treasurer's Office. He is working with Personnel with this position and it would be very helpful to have this person on board for this migration.
In the contract, People Soft is telling the County that it does take a lot of people and time to do the migration. Doug said when the City did the move to JDE in his mind Vince did it better than anyone else because Vince worked on it himself and had other people take over his normal duties.
The back up plan was to extend the contract with AMS and now they are being bought out by a Canadian company. So that fall back my go by the wayside?

Next Meeting:

April 8, 2004